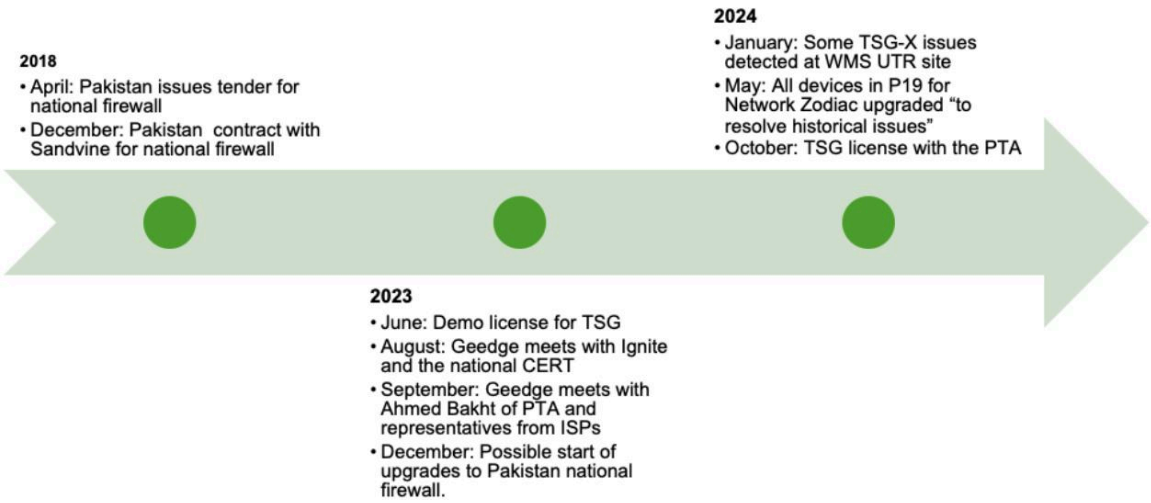
P19: Pakistan


2018
• April: Pakistan issues tender for national firewall
• December: Pakistan contract with Sandvine for national firewall
2023
• June: Demo license for TSG
• August: Geedge meets with Ignite and the national CERT
• September: Geedge meets with Ahmed Bakht of PTA and representatives from ISPs
• December: Possible start of upgrades to Pakistan national firewall.
2024
• January: Some TSG-X issues detected at WMS UTR site
• May: All devices in P19 for Network Zodiac upgraded "to resolve historical issues"
• October: TSG license with the PTA

Context

For many years, Pakistan's government has laid the groundwork for surveillance and censorship of its population. Access Now's Keep It On coalition began to register disruptions in Pakistan beginning in 2016.[44]

In 2024, Keep It On registered 21 shutdowns, the country's largest single number of shutdowns in one year. The Pakistan Telecom Authority's (PTA) 2024 annual report acknowledges over 100,000 instances of blocking of specific content.[45] According to their reporting, most of the sites were blocked for reasons of 'morality', 'national security', and 'incitement of hate on the basis of religion'; however, no precise definitions of these terms are provided under the law. Additionally, the Prevention of Electronic Crimes Act, 2016 enables the government to conduct mass and targeted surveillance. In 2013, Citizen Lab reported that Pakistan was using technology from a Canadian company Netsweeper to filter and block internet traffic.[46] In March 2018, the PTA issued a tender for a web management system (WMS) that would be "self-learning" and able to identify websites that were blasphemous or threatening national security.[47] Following this tender, Coda Story reported that Pakistan signed a $18.5 million contract in December 2018 with a second Canadian company, Sandvine, for a version of this system.[48] By reviewing records of shipment data, Amnesty International's Security Lab has concluded the shipments of technology for Sandvine's WMS began in 2017 and continued throughout 2022. [49] The first iteration of the Pakistan national firewall or WMS was using deep packet inspection to monitor communications on behalf of the telecommunications regulator, PTA.

(44) "EMBOLDENED OFFENDERS, ENDANGERED COMMUNITIES: Internet Shutdowns in 2024." AccessNow, February 2025. https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf.
(45) "Annual Report 2024." Pakistan Telecommunication Authority, December 16, 2024. https://www.pta.gov.pk/assets/media/2024-12-16-pta_annual_report.pdf.
(46) Poetranto, Irene. "Netsweeper in Pakistan." The Citizen Lab, August 1, 2013. https://citizenlab.ca/2013/08/netsweeper-in-pakistan/.
(47) "Replies to Queries Raised on Pre-Qualification Process for Web Management System." Pakistan Telecommunication Authority, March 20, 2018. https://pta.gov.pk/assets/media/response_queries_210318.pdf.
(48) Ali, Umer, and Ramsha Jahangir. "Pakistan Moves to Install Nationwide 'Web Monitoring System.'" Coda Story, October 24, 2019. https://www.codastory.com/authoritarian-tech/pakistan-nationwide-web-monitoring/.
(49) Amnesty International, "Shadows of Control", Amnesty International, September 9, 2025. https://www.amnesty.org/en/documents/asa33/020 6/2025/en/

Contd. P19: Pakistan

Pakistan and Geedge

Geedge's codename for their Pakistan project is P19. According to the evidence in the new documents, Geedge's operations in the country did not begin until 2023. This aligns with when Sandvine ended their contract with Pakistan in November 2023, responding to sanctions imposed by the United States Department of Commerce.[50]

The Geedge version of Pakistan's national firewall, which Amnesty International Security Lab calls WMS 2.0, includes new functionalities courtesy of TSG-OS. The modern firewall can store details about who is using a censorship circumvention tool and which IP-addresses visited which websites. It can monitor the internet traffic as well as telephone communications within the country and can track and block access to circumvention tools such as VPNs and specific websites.

The language used by a senior Pakistan ISP executive in an interview with Al Jazeera, mirrors Geedge marketing materials closely.[51] The unnamed executive said the new WMS was being deployed not only at the country's internet gateways but at local data centers of mobile service providers and ISPs.[52] Because the previous system was only able to surveil content entering and exiting the country, Pakistan was not able to censor content hosted by local caching content delivery networks (CDNs) like those run by Netflix and Meta. Comparing WMS 1.0 and WMS 2.0, the executive said: "Unlike the Sandvine system, the new DPI-based system is now capable of monitoring local internet traffic," using an "in-line network" which also had a higher likelihood of slowing down internet speeds for users. The executive also noted that the Chinese (Geedge) technology provides the capability to manage applications and websites at a "granular level", providing better features than Sandvine.

Unlike other countries using Geedge services, there are not national or regional centers in Pakistan. Instead, and likely a remnant of the old Sandvine system, Geedge is installed at three sites: PCAP (the generic term for data center and noted for "backup"), MSH (where most of the TSG hardware is), TWA (likely the Karachi Submarine Cable Landing Station owned by the company Transworld Associates).

(50) Effective February 28, 2024, Sandvine was added to the Entity List by the US Department of Commerce, subjecting it to enhanced export licensing requirements.
"The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses ." U.S. Department of State, February 28, 2024. https://2021-2025.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-abuses/. In November 2024 the sanctions were lifted, but Sandvine's time in Pakistan was coming to an end.
(51) As reported by Al Jazeera, Sandvine's contract with Pakistan, which began in 2018 and was set to end in 2023, was not renewed after a change of government in 2022. The new leadership opted instead to seek out a company that could provide more granular content filtering. (Hussain, "Pakistan Tests Secret China-like 'Firewall' to Tighten Online Surveillance," Al Jazeera, November 26, 2024, https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digitalhttps://www.aljazeera.com/news/2024/11/26/pakisan-tests-china-like-digital-firewall-to-tighten-online-surveillance)
(52) It should be noted that the Al Jazeera article does not name Geedge as the Chinese technology company related to the new WMS.

Contd. Pakistan and Geedge

Geedge Platforms on Old Hardware and Troubling Privacy Concerns

In their new report **Shadows of Control**, Amnesty International's Security Lab writes that one of the most important revelations from the leak of documents from Geedge Networks is "how technologies from different suppliers can be inter-dependent and repurposed to work together."[53] In other words, the system established by Sandvine became a foundation, and when their contract not renewed, Geedge was able to repurpose Sandvine's hardware to run the Geedge operating system. Amnesty found a document showing the design of the WMS, from July 20, 2023, running Geedge's TSG platform on repurposed Sandvine hardware.[54]

While built on repurposed hardware, a report in Al Jazeera hints at how much the Geedge system might have cost: officials who spoke to the Qatari news broadcasters on condition of anonymity said that a new Chinese system from an unnamed supplier would cost Pakistan between 20 to 30 billion rupees ($72 million to $107 million), and was responsible for the slower internet speeds and full-on shutdowns reported by users in the second half of 2024.[55]

The Geedge system can capture more than metadata. If a connection is unencrypted, the system will also opportunistically capture the content. Amnesty International found one support ticket in Geedge's Jira system with the full content of two emails including attachments and the e-mail password, which was intercepted by TSG on an unencrypted connection to an email server.[56]

It is concerning that sensitive user data is included in a support ticket for a third-party service provider, and that this sensitive data was part of a leak. To further illustrate the troubling issues of user data and privacy within the Pakistan case, as Amnesty points out, since 2015 every new SIM card issued to a mobile subscriber in the country must be registered to a particular user and linked to biometrics including fingerprints that are registered via the National Database and Registration Authority (NADRA). People need a NADRA profile to access basic services like healthcare, banking, and education. The NADRA profile also links to other databases, like voter registration and tax records, which combined create a comprehensive record on every citizen. [57] A core feature of Geedge's Sanity Directory component is attributing traffic to a specific SIM card. This enables, not only mass surveillance, but highly targeted micro-surveillance on specific individuals in Pakistan and other countries Geedge operates.

(53) Amnesty International, "Shadows of Control".
(54) Amnesty International, "Shadows of Control".
(55) Hussain, "Pakistan Tests Secret China-like 'Firewall' to Tighten Online Surveillance," Al Jazeera, November 26, 2024, https://www.aljazeera.com/news/2024/11/26/pakisan-tests-china-like-digital-firewall-to-tighten-online-surveillance
(56) Amnesty International, "Shadows of Control".
(57) Amnesty International, "Shadows of Control".

Contd. Geedge Platforms on Old Hardware and Troubling Privacy Concerns

From the Pakistan case, we can learn how adopting Geedge's system greatly enhanced the government’s surveillance capabilities, giving them a new capacity to monitor local internet traffic and track the use of circumvention tools. The repurposing of Sandvine's hardware by Geedge highlights the company's ability to adapt and use existing infrastructure, and their willingness to take advantage of sanctions against a competitor as a market opportunity. Furthermore, the integration of TSG-OS with biometric data from SIM card registrations highlights that the Geedge system can be combined with other surveillance systems, creating an even more comprehensive monitoring framework.